Acano solution 1.6

Solution Support FAQs

Acano

January 2015

76-1022-08-K

Contents

1 Interoperability 4
Which video endpoints has the solution been tested with? 4
Which call control platforms has the solution been tested with? 4
Which LDAP server has the solution been tested with? 4

2 Acano X Series Server 5
Does Acano provide a software or hardware solution? 5
Can the Acano X series server also run on DC power? 5
What is the average power consumption of the Acano X series server? 5
What heat output does the air conditioning need to cope with? 5
What is the form factor of the Acano x86-based servers? 5
Does the Acano X series server contain DSPs, FPGAs or other application-specific processing hardware? 6
Can I replace the fan tray module in the Acano X series server? 6
Can the supplied rack ears support the Acano X series server? 7
What operating system is used on the Acano X series server? 7
What do the Status LEDs mean on the Acano X series server? 7
My Acano X series server came without rack rails; can I get rails for it through Acano? 8
Is it a requirement to have DNS configured on both the Admin and A to D interfaces? 8
Is the Acano X series server RoHS compliant? 8

3 Acano X Series Server and Virtualized Deployments 9
What are the recommended DNS records to create? 9
How many CDRs can the Acano solution store? 9
Which ports need to be opened? 9
Which Syslog server should be used? 9
I can't connect to my Syslog server; what should I check? 9
What is the Admin login account recovery process? 9
What's the difference between the MMP and application interfaces? 10
I cannot reach the web interface, what should I check? 10
Does Acano support SRTP on 3rd party SIP clients 11
I cannot get encrypted SIP calls to work 11
Does the Acano solution support multi-tenancy? 11
How does multi-tenancy affect user experience? 11
How do I back up (and restore) the Acano solution configuration? 12
How can I back up the Acano solution configuration automatically? 13
Can I use the same certificate on two Acano services? 14
Can I use wildcard certificates? 14
Does the Acano solution require a chain of intermediate certificates between the Call Bridge certificate and the root CA certificate? 15
When I download certificates from my Certificate Authority, it asks for the server type. What should I select? 15
Can I integrate the Acano solution with more than one Lync server? 15
Calls to Lync fail to connect and the error shown in Lync logs show "The peer is using a wildcard certificate but did not identify itself with a NEGOTIATE request" 15
I have multiple Acano servers using the same Lync environment: do I need multiple accounts for the Lync Edge settings to use? 15

What factors impact the resolution Lync clients send to and receive from the Acano solution? 15
Why do I need the UDP port range 50000-59999 open across the firewall for calls from a Lync client when using the Acano solution? 16
Can calls between SIP endpoints and Lync users be hosted on the Lync AVMCU? 16
Should I see the LDAP server configured on the Web Admin Interface in the API? 16
How do I import a security group from the Active Directory server using the API? 16
I cannot log in using an Acano client in a deployment with separate Acano Core and Edge servers because authentication fails. What should I check? 19
I suspect a firewall issue stopping WebRTC. Can I check this? 19
Why isn't a coSpace Call ID dialable? 19
I want Acano users to be able to enter a +E.164 number and no @domain suffix to dial out, how can I configure the Acano dial plan to do this? 19
Does the Acano solution support SNMP? 20
Are there settings to level out the volume of the various endpoints? 20
How stable is the Call Bridge? 20
Does the Acano solution support both AES and SIPS, and conform to the ISO/IEC 18033-3 standard? 20
How long does the Acano solution take to boot or restart? 21
How can I use the Secondary URI field? 21
Upgrade fails because the upgrade image failed to mount 21
Tips for making Multiway calls 21
Does the Acano solution support multiple domains? 21
Troubleshooting Web Bridge connectivity issues 21
I see following error message when trying to add a Call Bridge: "Parent IM domain <example.com> of domain <callbridge.example.com> does not exist". What is wrong? 22
How do I set up "Lecture mode"? 23
How do I set up host and guest access? 24
How do I enforce encryption for a coSpace? 24
I see that different members of the same coSpace can have different permissions on that coSpace. How does this occur? 25
How do I set the default layout for every coSpace? 26
What information is included in the email invitation? 26
What does "RTCP unprotect authentication failure" in the event log mean? 26
How do I move the master database? 26
Does Acano support Skype integration? 27
What is the minimum bit rate for audio and video? 27
Is TIP supported in R1.6 and on what systems? 27
In release 1.6, can I have one Edge server for two Core servers? 28

4 Virtualized Deployments 29
What VM host server should I use? 29
Which versions of the hypervisor are recommended? 29

Note: There is a separate FAQ document for the Acano clients at www.acano.com/help/.

1 Interoperability

Which video endpoints has the solution been tested with?

Acano supports common standard-based endpoints and call control platforms such as:

- Cisco MXP (v F9.1 or higher)
- Cisco C-Series (v TC 5.1 or higher)
- Cisco EX (v TC 5.1 or higher)
- Cisco E-Series (v TE 4.1 or higher)
- Jabber (v 4.6 or higher)
- Polycom HDX-Series (v 3.1.2 or higher)
- LifeSize 220 Series (v4.11 or higher)
- LifeSize Room (v4.7 or higher)
- Lync 2013 & 2010 clients on MAC & Windows PC
- CTS 3000 version 1.10.1(43)
- Lync Room systems

Which call control platforms has the solution been tested with?

- Cisco Unified Communication Manager (CUCM). We have only tested with v 9.0 but expect other versions to work. We will do our best to support other versions but we don't actively test with them
- Cisco VCS Expressway or Control (V X6.1 or Higher)
- Lync 2013 & 2010
- Avaya Communication Server (v 6.5 and Higher)
- Acme Packet Net-Net 3820 SCX6.4.0

Which LDAP server has the solution been tested with?

Active Directory and OpenLDAP are the only supported LDAP servers currently. We have had success with Samba but we have not officially tested and verified that all functions work with it. We hope to support more LDAP servers in the future.

Which Lync Server versions has the solution been tested with?

We support Lync Server 2010 and Lync Server 2013.

Does the Acano solution support OCS?

No, and there are no plans currently to do so.

2 Acano X Series Server

Does Acano provide a software or hardware solution?

The Acano solution comprises a number of software modules that can run on top of an Intel x86-based platform for the complete solution which is called the Acano X series server deployment in the documentation. Acano supplies both software and the x86-based servers for the Acano X series server deployment.

A virtualized deployment is also available.

Can the Acano X series server also run on DC power?

The Acano X series server has been designed to use a DC power supply module as well as the currently supplied AC power supplies. The DC power supply will be provided as an option, contact your Acano sales representative for details.

The DC supplies will be a plug-in module of exactly the same size as the AC module. The input voltage range is 40 - 72V and it will have all the expected over voltage and regulation features, as well as load balancing on the internal power bus.

What is the average power consumption of the Acano X series server?

We don't publish an average power consumption figure. The product Hardware Datasheet specifies a maximum power figure of 1000W for X3, X2 and X1 (all three models have the same power supply). The actual consumption at any time will be dependent on a great many factors so it is not possible to provide an average value for you. You may well indeed be seeing a much lower value than 1000W reported in the Syslog in tests you are doing at the moment. We would advise provisioning for the value given in the datasheet to allow for the possibility that future software updates will change the performance of the hardware and result in a corresponding change in power consumption.

What heat output does the air conditioning need to cope with?

When provisioning air conditioning for the X series server allow for the following heat output from each model.

Model	BTU/h approx.
X1	1706
X2	2559
X3	3412

What is the form factor of the Acano x86-based servers?

The Acano X series server is a 2U high, 19" rack-mountable box.

Does the Acano X series server contain DSPs, FPGAs or other application-specific processing hardware?

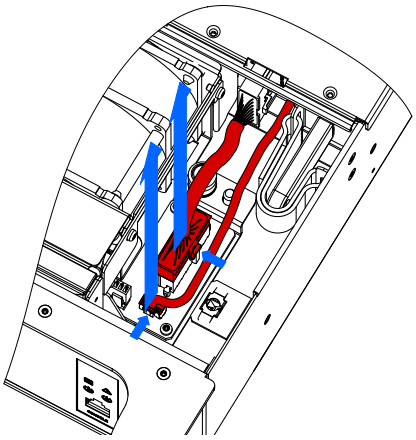
No, the Acano X series server is based on standard Intel x86 CPUs, with PCI-express interconnect and Intel network interface cards.

Can I replace the fan tray module in the Acano X series server?

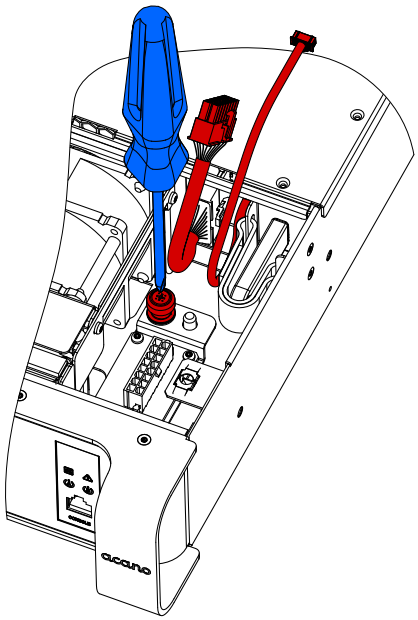
Yes this is a user-replaceable part. Follow these steps in order.

1. At the back of the Acano X series server, unplug both power units
2. Using a Philips screwdriver unscrew the service hatch on the top of the Acano X series server.
3. Push in and then lift out each of the two connectors shown on the right.

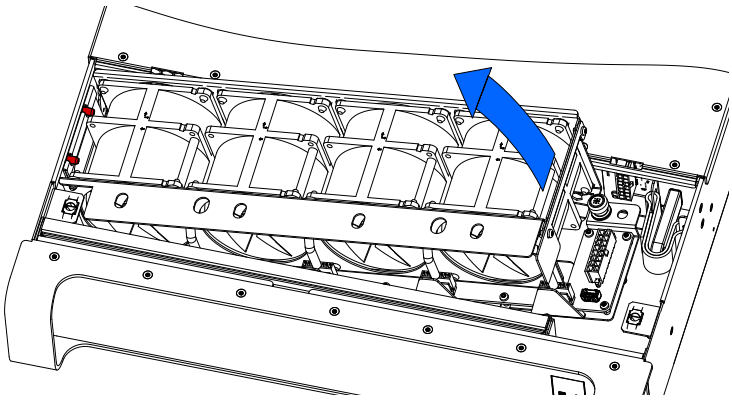
   Fold back the cables.



4. Unscrew the fan tray module as shown.



5. Lift out the module.



6. Insert the new fan tray module by reversing the steps above.

Can the supplied rack ears support the Acano X series server?

Definitely not! The Acano X series server must be supported on the rack rails supplied by Acano. The rack ears are not designed to be load-bearing and therefore Acano can take no responsibility for the server or any other equipment if the rack ears are the only support.

What operating system is used on the Acano X series server?

The Acano X series server runs on a Linux-based platform created specifically for our product. This provides a minimally complex platform environment that can be monitored for security, performance and stability using our secure development life-cycle.

What do the Status LEDs mean on the Acano X series server?

The Acano X series server has status LEDS on both the front and back panels. (

Front

OK

- Blue: normal operation

Warning

- If on (red), check the cause urgently in the Web Admin Interface **Status > General** page.

Supply A/B

- Blue: power supply is operating normally
- Flashing quickly: power supply is present but not functioning (i.e. not plugged in)
- Flashing slowly: power supply is not present

Note: If either power supply LED is flashing; check the cause urgently in the Web Admin Interface **Status > General** page.

Back panel LEDs

All five Ethernet ports (Admin and A to D) have the same LED behavior:

- Left
  - Green: Link at 10G
  - Amber: Link at 1G
  - Off: Link at 10/100M
- Right
  - Green: Link up
  - Blinking: Activity on link
  - Off: Link down

My Acano X series server came without rack rails; can I get rails for it through Acano?

No, although new Acano X series servers ship with rack rails, these rack rails do not fit the older Acano X series server casing. Older Acano X series servers must be placed on a rack shelf.

Is it a requirement to have DNS configured on both the Admin and A to D interfaces?

We recommend using DNS on both interfaces. Currently, you must have DNS working on the application interface(s) A to D. It may be possible for the Acano solution to work without a configured DNS server on the Admin interface so long as you have configured Syslog and NTP servers with IP addresses.

Is the Acano X series server RoHS compliant?

We meet the European RoHS directive.

3 Acano X Series Server and Virtualized Deployments

FAQs in this section apply equally to Acano X series servers and VM-hosted servers.

What are the recommended DNS records to create?

The latest information is in Appendix B of each Deployment Guide.

How many CDRs can the Acano solution store?

There is no persistent storage of CDRs on the Acano servers; CDRs are streamed to the CDR storage receiver. They are temporarily buffered on the server and when they have been sent to the receiver they are removed.

Which ports need to be opened?

The latest information is in Appendix B of each Deployment Guide.

Which Syslog server should be used?

We have tested with http://www.solarwinds.com/kiwi-syslog-server.aspx

I can't connect to my Syslog server; what should I check?

Ensure you have set up an open port between the MMP and the Syslog server as a TCP port on port 514 (not UDP).

What is the Admin login account recovery process?

On a VM-hosted server you must have at least two admin level accounts at all times: then if you lose the password for one account you can still log in with the other one and reset the lost password. We recommend that you create two new accounts and then delete the default "admin" account; because the username "admin" is not very secure. There is no way to reset an account's password if you cannot log in.

On an Acano X series server, follow the steps below if you have lost the password on any admin account on the MMP and are unable to log in. This process resets the admin login account and does not lose any of the configuration data.

1. Using a Philips screwdriver loosen the two screws on the top front service hatch and hinge the cover upwards.

   You see the fan module on the left and a smaller area on the right with cables and connectors. In this area and behind the front grill are two small buttons: one red and one black.
2. Carefully press the **red** button only.
3. Within 4 minutes of pressing this button log into the Acano X series server using the Console port and serial cable provided: user account is "admin", no password will be requested.

4. Set up your new admin account using the following command.

   ```
   user add admin admin
   ```

5. You will then be prompted for a password which you will have to enter twice.
6. Close the hatch and push the screws down to secure the hatch, no screwdriver is needed.

Note: When you log in subsequently, either via the Console port or Admin interface, using the admin account you will be asked for this password.

What's the difference between the MMP and application interfaces?

There are two layers to the Acano solution: a Platform and an Application.

- The Platform is configured through the Mainboard Management Processor (MMP). The MMP is used for low level bootstrapping and configuration. It presents a command line interface

  Note: On the Acano X series servers the MMP can be accessed via the serial Console port or using SSH on the Ethernet interface labeled Admin. In the virtualized deployment the MMP is accessed on virtual interface A.

- The Application runs on this managed platform with configuration interfaces of its own. The application level administration (call and media management) is done either via the Call Bridge's Web Admin Interface (which can be configured to run on any one of the Ethernet interfaces) or via the API

  On the Acano X series servers there are five physical Ethernet interfaces labeled Admin, A, B C and D. In the virtualized deployment one Ethernet interface (A) is created but up to three more can be added (B, C and D).

  Note: There is no physical separation between the media interfaces A-D on an X series server but the Admin interface is physically separate. Each interface is configured independently of the others at the IP level. IP forwarding is not enabled in either the Admin or host IP stack.

I cannot reach the web interface, what should I check?

Check the following:

1. Check that the certificates have been copied ok.

   When you SFTP into the file system of the server do you see the certificates listed with the other files?

   Note: if you are using a Windows PC we recommend WinSCP

2. Check the certificates.
   a. Double check that each certificate has created correctly, and uploaded along with the matching key.
   b. Both the certificate and the key file need to be in PEM or DER format.

c. Check the file extensions: the certificate can have a .crt, .cer, .pem and .der extension, and the private key needs a .pem, .der or .key extension.

d. File names can contain alphanumeric, hyphen or underscore characters.

e. Ensure that you have the correct certificate to go with the corresponding key, otherwise it will not work. Use the MMP command pki match <key> <certificate> to check.

3. Check the Web Admin Interface configuration.

   Log in to the MMP and type `webadmin`. Are the certificate/key names exactly the same as the files you uploaded, including file extension?

   Check that Web Admin Interface is enabled and listening on the MMP, by typing the following in the MMP:

   ```
   webadmin enable
   webadmin listen mmp 443
   ```

4. Check that you have access via IP.

   Try accessing the web interface just using IP i.e. in a browser type

   `https://<ip address>:<port #>`

Does Acano support SRTP on 3rd party SIP clients

Yes, we call it Encryption – see the next FAQ.

I cannot get encrypted SIP calls to work

Check the following:

- That in the Web Admin Interface **Configuration > Call Settings** page, SIP Media Encryption is set to Allowed or Required
- That you have uploaded a certificate and private key for the Call Bridge
- That you have the Call Bridge configured to use that certificate and private key

The Acano solution will only encrypt media when using TLS for call control and if SIP Media Encryption is set to Allowed or Required. If it is using TCP or UDP for call control, or if SIP Media Encryption is set to Disabled, no media encryption will be used for calls.

Does the Acano solution support multi-tenancy?

Yes, it does. This refers to sub-dividing its capacity into a set of “islands” where each island has all of the functionality of the whole, but has no access to the resources (for instance users, coSpaces, or active calls) of other tenants. The API is the primary means by which tenants are supported. See the Acano Solution API Reference Guide for full details.

If you use different domain names to distinguish between customers, such as those below, you must use the multi-tenancy functionality.

- meetingroom1@customerA.com
- meetingroom1@customerB.com

How does multi-tenancy affect user experience?

There are different behaviours when calling from one deployment to another.

- If two deployments are separate, then the call is a SIP call and the list of participants displayed on the Acano client in-call doesn't work. For example, you can call 8945089873.coSpace@examplecompany.com from an Acano client connected to your deployment to join a call on examplecompany's server.
- The better experience is when the two deployments are tenants on the same Acano solution. The full experience is preserved even though the two tenants have no visibility of each other's data in searches.

For example:

Partner X Tenant A user:

- Can join Partner X Tenant B user's meeting via their Acano PC/Mac/iPad/iPhone Client when logged in and can see the list of participants
- Can only see Partner X Tenant A Contacts when searching People
- Can only make point-to-point video calls with other Partner X Tenant A Contacts in the People Directory, assuming they are online
- Can join Partner Y Tenant 1 user's meeting via their Acano PC/Mac/iPad/iPhone Client when logged in but cannot see the list of participants
- Can call a Partner Y Tenant 1 user — if the direct dial URL is known

How do I back up (and restore) the Acano solution configuration?

There are two MMP commands that allow you to back up the complete system configuration in a file that can be downloaded using SFTP, and restored if necessary.

- backup snapshot <name>. This command creates a full system snapshot in the file <name>.bak (including, IP addresses, passwords and certificates)
- backup rollback <name>. This command restores the system from the file, overwriting the existing configuration and rebooting the Acano solution. Therefore a warning message is displayed and you must confirm your action.

Note: It is not possible to create a backup from one type of deployment (Acano X series server or virtualized) and roll it back on the other type.

When you restore from the backup, everything is overwritten including the IP address, certificates and the license.dat file. Therefore if you are restoring onto a different server from the one that the backup was made on and the "destination" server had a permanent license:

1. Store a copy of its license.dat, VM license (If appropriate) and certificates.
2. Restore the backup on to it.
3. You now have the same files on both servers. Manually replace the restored version of license.dat with the saved copy, otherwise the Acano solution will not work because:
    - The VM activation license is tied to the MAC address of the port A interface
    - The XMPP license, which is required for both Acano X series server and virtualized deployment, is tied to the MMP or port A interface
4. Copy back the certificate and the VM license (if appropriate).

How can I back up the Acano solution configuration automatically?

We do not support any file share protocols; therefore, you must set up automatic backup externally. This FAQ provides one example of how to do this in the following releases 1.1, 1.2 and 1.6.x where x≥7.

Requirements

A laptop, desktop PC or a VM with low resources e.g. 2 cores, 2Gb RAM and enough storage: a demo server with over 2,000 coSpaces and over 3,000 users on it creates backups that are approximately 4Mb each.

A login account that is used frequently so that the password is updated regularly; then expired passwords will not cause backup failures.

Steps

1. Download Linux Distro of your choice, we prefer Ubuntu Server which can be downloaded from: http://www.ubuntu.com/download/server.
2. Install with default settings; when asked for Extra Items, select **OpenSSH Server** so that remote login is possible via SSH immediately after install.
3. Install OpenSSH if it is not installed on OS Install (using `sudo apt-get install openssh-server`)
4. Perform Ubuntu updates as required using `sudo apt-get update`, `sudo apt-get upgrade` and `sudo apt-get dist-upgrade`.
5. Create an SSH Key with `ssh-keygen -t rsa` and press **Enter** when asked for the Name and Passphrase (so that the command uses the default name and no passphrase).
6. Use SCP (such as WinSCP) to connect and copy the newly created SSH Key from the server (from the /home/useraccount/.ssh folder).
7. Rename the locally saved SSH Key to <configbackup>.pub (where configbackup is the login name created below).
8. Create a user account on the Acano server using the MMP command `user add configbackup admin` and enter a password for this account twice.
9. Use SFTP to connect to the Acano server and copy the <configbackup>.pub SSH Key to the Acano server.
10. Log in to the Acano server from the Ubuntu PC using SSH and accept the SSH key (i.e. use `ssh <loginaccount>@<acanoserver.ip address>` and press **Y** to accept the SSH key when prompted).
11. Verify that the login above was successful without needing to enter password (because the SSH Key should have allowed login after pressing **Y**).
12. Write a backup script and copy the script to your home folder or preferred location. Edit it as needed for your directory path and server details.
13. Add a cron job to execute the script at an appropriate interval (using `crontab -e`)
14. Manually execute the script to test that it works from within the directory that the script is located in (using `./ServerBackup.sh` assuming that the script name is ServerBackup.sh)

Below is an example script and cron job.

Example script

This script logs into the Acano server at 192.168.10.21 using a login account called "configbackup". It then issues the backup snapshot command to create a backup called ServerBackup. It then logs out of SSH and logs in again with SFTP using the same username, and copies the ServerBackup.bak file storing it locally at the path /home/acano/configbackups with the name ServerBackup_year-month-day.bak (e.g. ServerBackup_2014-7-10.bak).

Edit the script as needed for the Acano server IP address, login details and folder path to the local server (as well as backup names, if ServerBackup is not ideal).

```
#!/bin/bash

ssh configbackup@192.168.10.21 << !
backup snapshot ServerBackup
!

sleep 5

sftp configbackup@192.168.10.21 << !
get ServerBackup.bak /home/acano/ServerBackup_$(date +%Y-%m-%d).bak
bye
!
```

Example cron job

When added using `crontab -e` this cron job will run the script at /home/acano/ServerBackup.sh at 1:00 AM local time as set on the Linux PC.

```
0 1 * * * /home/acano/ServerBackup.sh
```

Can I use the same certificate on two Acano services?

While it is possible to use the same certificates on two services, it is not recommended. Certificates have a CN field which is for the Common Name: this should match the service's FQDN and should be the name you use to access it. If this is not the case, most services will complain and display certificate warnings.

For internal services such as the Web Admin Interface, this is not really an issue, and the errors can be dismissed. However, for external services such as WebRTC, this normally causes people concern because they do not know whether they should trust the website or not.

Therefore we suggest using a unique certificate for every service. However, see the next FAQ.

Can I use wildcard certificates?

Yes, except for Lync which rejects them when presented – see the next FAQ.

Wildcard certificates cost more but can be used on multiple servers. In these wildcard certificates, you can define the CN field to be *. example.com for example and then any server that is named something. example.com will be matched as correct for this CN. This allows you to put the certificate on emailserver. example.com, webserver. example.com, ftpserver. example.com, etc. and use just this one certificate.

However, there are some limitations; in the example above anything named beyond that scheme will not work, such as acano.video. example.com.

In terms of usage wildcard certificates are created, authorized and uploaded as normal.

Does the Acano solution require a chain of intermediate certificates between the Call Bridge certificate and the root CA certificate?

If your SIP Call Control device is a Lync Server, you should not need the full certificate chain installed if the Lync server trusts the Call Bridge certificate. The best way to do this is to create the Call Bridge certificate on the Lync server domain. The reason is that, unlike the Lync server, the Call Bridge does not accept TLS connections from the Lync clients (only from the Lync Server).

However, you may need the complete chain of certificates if you are using other Call Control devices.

When I download certificates from my Certificate Authority, it asks for the server type. What should I select?

When submitting your certificate request through your CA provider and asked for the server type, select one of the following: Generic Webserver, Other or Apache. Certificates should be Base64 encoded and uploaded to the Acano server per the instructions in the Installation Guides and Deployment Guides.

Can I integrate the Acano solution with more than one Lync server?

There is support for multiple Lync integrations per Acano solution; the only limitation is that you can only use the Lync Edge server from one of the integrations. This is the only part of the Lync integration that is 'per Call Bridge'; otherwise you can create trunks to as many different Lync Front End servers as required.

Calls to Lync fail to connect and the error shown in Lync logs show "The peer is using a wildcard certificate but did not identify itself with a NEGOTIATE request"

We believe Lync does not handle certificates that have a wildcard entry as the CN very well. Re-create the certificate using the FQDN of the Acano server as the CN. This does not need to be a public certificate in most cases: create a signed certificate with OpenSSL or a Microsoft CA server. Then upload the CA's Public Key to the Lync FE Server's Trusted Root Certification Authorities folder.

I have multiple Acano servers using the same Lync environment: do I need multiple accounts for the Lync Edge settings to use?

This should not be an issue at all because the Acano solution does not log into the Lync server.

What factors impact the resolution Lync clients send to and receive from the Acano solution?

To have HD calls with Lync (either 2010 or 2013) using RTV, you need a Quad Core CPU.

What Lync sends to the Acano solution is a function of Lync, the camera and CPU capabilities (among other things). Window size is also a factor here.

What the Acano solutions sends to Lync is a function of what video we have to send to Lync and what Lync client says that it wants to receive. Lync sends us “Size Hints” during a call that tells us what it wants to receive: if it is telling us to only send 640x480, the Acano solution must obey this.

With Lync 2013, you will only get 720p if the Lync window is full-screen. If opened as small window or even Maximized, it will only tell us to send 4x3 resolution @ 640x480. Therefore for HD ensure that you have clicked the **Full Screen** button.

Also, only in Lync 2013, screen resolution can make a big difference. In most cases with Lync 2010, we can get 720p on most Full Screen calls as long as the screen is set to a resolution of 1280x720 or greater. However, in Lync 2013 and using the same PC, it has been observed that screen resolutions of 1280x800 or higher are required to get the Lync client to request 720p in calls.

Why do I need the UDP port range 50000-59999 open across the firewall for calls from a Lync client when using the Acano solution?

Lync clients have the ability to send media to the Lync Edge server over a TCP connection to port 443 or over UDP in the 50000-59999 range. However, the Acano solution only supports UDP for audio and main video (because this is preferable to TCP for several reasons). Therefore the ports need to be open to allow the Lync client to use UDP.

Can calls between SIP endpoints and Lync users be hosted on the Lync AVMCU?

In R1.6, multipoint calls between SIP endpoints and Lync users can be hosted on the Lync AVMCU, using the Acano server as a gateway. No special configuration is needed; just the standard Lync integration configuration working as detailed in the Acano solution Deployment guides. If you want to use this setup for external and federated Lync users also, you must enable the Lync Edge Integration and make sure that you set up Lync Federation correctly, and open the correct UDP and TCP ports for that as described in the Ports Used appendix of these Deployment guides.

Should I see the LDAP server configured on the Web Admin Interface in the API?

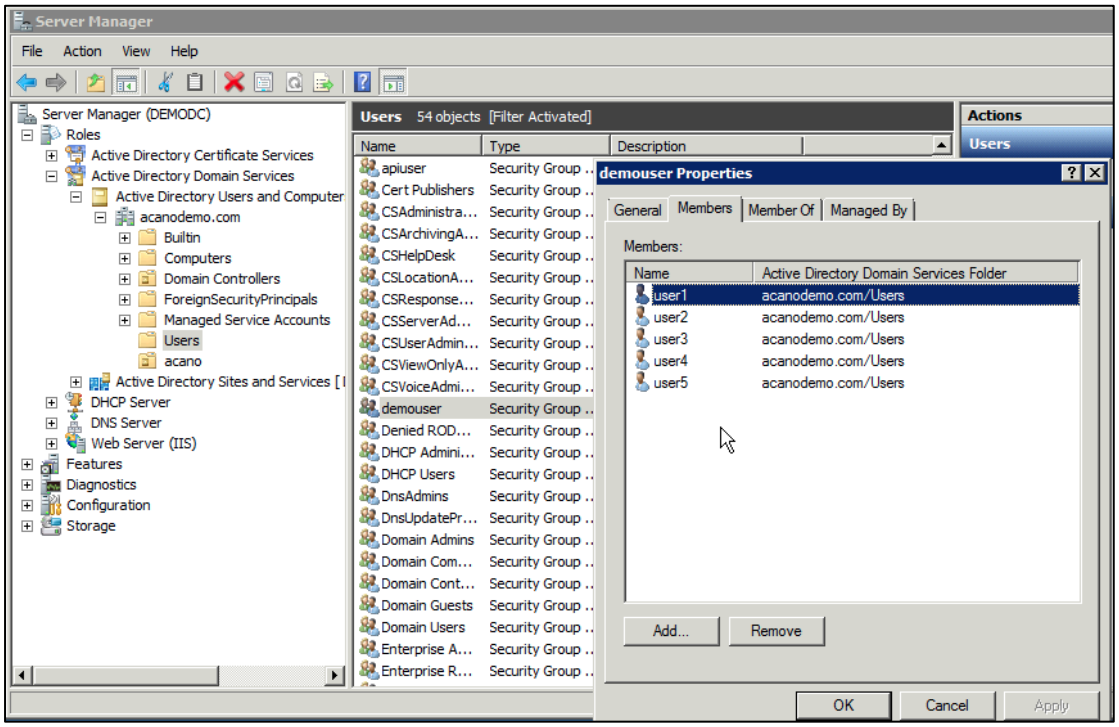
The Web Admin Interface-configured LDAP server works slightly differently to those configured via the API, and is only recommended for simple deployments and testing. If you are interested in multi-tenancy then we recommend that you remove the configuration from the Web Admin Interface **Configuration > Active Directory** page and use the API to configure LDAP imports. From R1.1 can use either the API or the **Sync now** button at the bottom of the **Configuration > Active Directory** page to synchronize the LDAP servers.

How do I import a security group from the Active Directory server using the API?

1. Create a security group on the Active Directory Server and add some users to the group.
2. On the Directory information tree structure, create ldapServers, ldapMappings and ldapSources using the Acano solution API. (See the API Reference guide for details.)

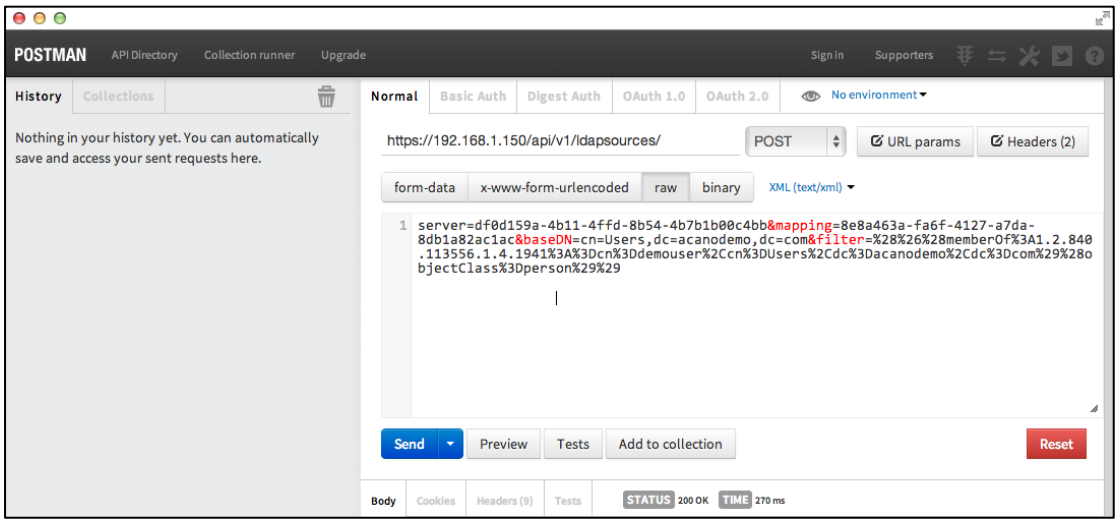
   When posting ldapSources, a POST URL format has to be used: see the following example.

In this example, Active Directory in Windows Server 2008 R2 64bit and Postman are used.



To import users from a security group called “demouser” with baseDn (cn=Users, dc=acanodemo, dc=com), we suggest the filter (see over page):

```
(filter=%28%26%28memberOf%3A1.2.840.113556.1.4.1941%3A%3Dcn%3Ddemouser%2Ccn%3DUsers%2Cdc%3Dacanodemo%2Cdc%3Dcom%29%28objectClass%3Dperson%29%29)
```



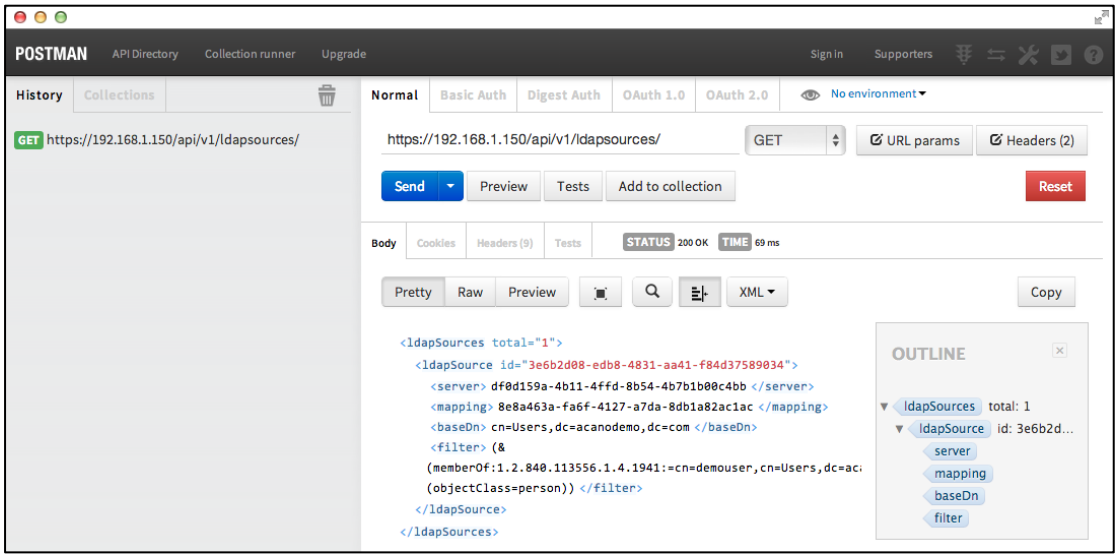
Note: Entering the same filter through a user interface and by using the API requires slightly different strings. Using the example above:

Filter on web page:
```
(&(memberOf:1.2.840.113556.1.4.1941:=cn=demouser,cn=Users,dc=acanodemo
,dc=com)(objectClass=person))
```

Filter through API:
```
%28%26%28memberOf%3A1.2.840.113556.1.4.1941%3A%3Dcn%3Ddemouser%2Ccn%3D
Users%2Cdc%3Dacanodemo%2Cdc%3Dcom%29%28objectClass%3Dperson%29%29
```

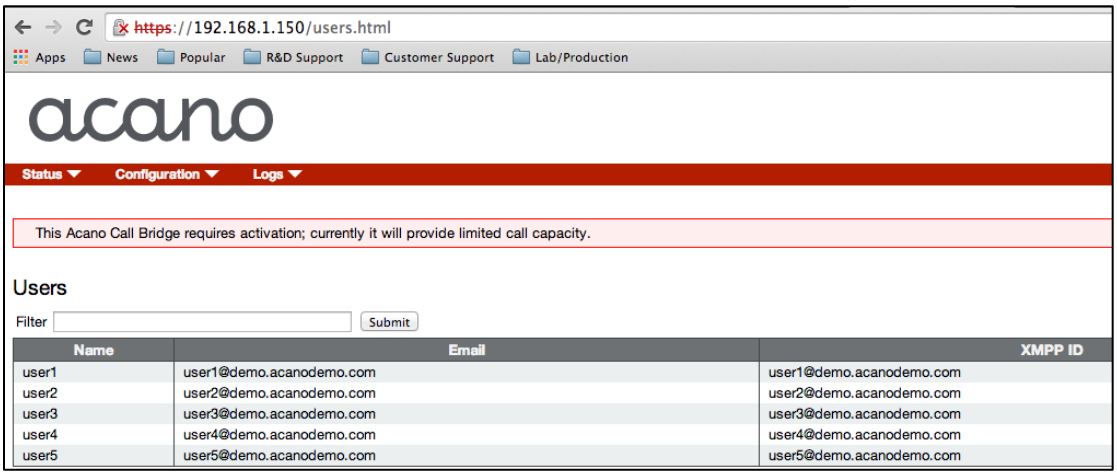
The following output of GET should be seen.

```
<filter>(&(memberOf:1.2.840.113556.1.4.1941:=cn=demouser,cn=Users,dc=ac
anodemo,dc=com)(objectClass=person))</filter>
```



3. Start a Sync either using the API or the Web Admin Interface.

   Users who are members of the security group are imported to Acano solution are shown in the Web Admin Interface **Status > Users** page as below.



If users are not imported, try the following:

4. If possible, delete all LdapSources through the API, configure these sources using the Active Directory Web interface, and then check if users are imported when synchronizing.
5. If first method is not possible, modify the filter to be a simple one; for example, “objectClass=person” and try to import users from an OU. This will confirm that the issue is with the filter.

I cannot log in using an Acano client in a deployment with separate Acano Core and Edge servers because authentication fails. What should I check?

The first thing to check is that the appropriate ports are open on both firewalls:

- External to DMZ firewall
- DMZ to Internal firewall

See Appendix B of the Acano solution Deployment Guide for a full description of the Acano solution’s port requirements. The document is available from the Partner web site.

I suspect a firewall issue stopping WebRTC. Can I check this?

In a browser type https://apprtc.appspot.com/. Then open another tab, and type chrome://webrtc-internals/ which will show ICE information.

Why isn’t a coSpace Call ID dialable?

A feature of the Acano Call Bridge is that it supports one or more dial in PSTN phone numbers for the IVR, and also supports connections via the Web Bridge. In both of these cases, to be able to join a coSpace you need to enter the ID for the coSpace that you want to join.

In a multi-tenant environment, it is not possible to determine which tenant you are calling from (or connecting from) in these cases. This means that the call ID you use has to be unique on the Acano Call Bridge so that the coSpace does not clash with any other coSpace for any configured tenant. Dialable IDs (URIs) for coSpaces aren't as restricted because the domain of the URI determines which tenant the call is for: multiple tenants can use "test.cospace" for example, because this might be dialed as "test.cospace@company1.com" for one tenant and "test.cospace@company2.com" for another tenant.

I want Acano users to be able to enter a +E.164 number and no @domain suffix to dial out, how can I configure the Acano dial plan to do this?

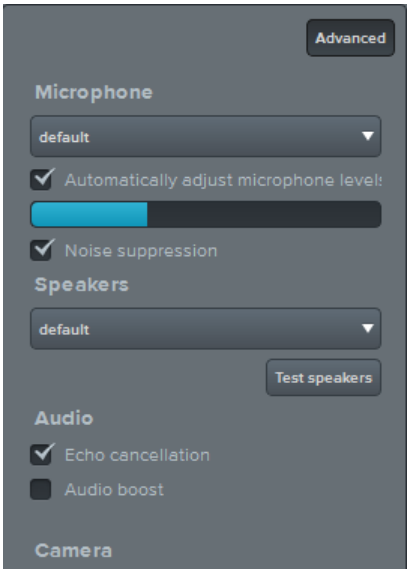
Enter a “match all” dial plan rule. Assuming that all of your current outbound dial plan rules have a domain entered, enter one additional rule with the lowest priority with nothing in the Domain field. This creates a “match all domains” rule.

Set it to the IP of your proxy server. For example if the “match all” rule is set to use 10.10.20.20 as the SIP Proxy to Use and the user dialed 12345, the call would go out to that proxy as 12345@10.10.20.20. How the proxy then handles the call is outside the scope of Acano.

Does the Acano solution support SNMP?

Yes, The Acano solution supports SNMP v1 traps but the MIB can be read with SNMP versions 1/2c and 3. The configuration is different for each. Be aware of the security implications of using SNMP version 1/2c: it does not support robust authentication and therefore anyone who knows the community string can query the server. See the MMP Command Reference Guide for full details. The MIBs are available on the Acano web site Support page or can be downloaded by SFTP from the Acano X series server/virtualized deployment.

Are there settings to level out the volume of the various endpoints?



No, there are no Acano server settings. However the PC Client and Mac Client allow you to adjust the gain of the microphone and speaker so you can control these endpoints.

See the Automatically Adjust Microphone Level and Audio Boost fields.

How stable is the Call Bridge?

A great deal of work has gone in on the Acano solution to avoid the Call Bridge restarting and therefore maintaining calls. A crash with code running on the media modules, where traditionally crashes occur on other products, will only impact calls on the module that crashed and does not restart the Call Bridge. The Call Bridge would only usually choose to restart itself in exceptional circumstances such as detecting that it was unable to service existing calls or to make new ones.

Does the Acano solution support both AES and SIPS, and conform to the ISO/IEC 18033-3 standard?

ISO/IEC 18033-3 is Part 3 of a document covering cryptography and only applies to the specification of certain block ciphers - of which AES is one.

SIPS can use AES but SIPS is outside of the scope of this standard.

We conform to the specification of AES as presented in ISO/IEC 18033-3, but our efforts at validation are towards FIPS. FIPS 140-2 validation of our cryptography module will be complete in Summer 2014.

How long does the Acano solution take to boot or restart?

It takes approximately 5-6 minutes to fully boot up. It can seem as if it is fully booted because the MMP (Admin interface) is accessible after a minute or so; however, the rest of the system is still booting and you cannot access the Web Admin Interface until it is fully booted. On the Acano X series server, if you see the red light on the front panel during this period, it is not an issue.

How can I use the Secondary URI field?

In R1.1 you can configure a secondary numeric URI for a coSpace. This can be done manually on individual coSpaces in the Web Admin Interface or automatically during an LDAP import using the API. (Note that the Acano clients do not show, and cannot set, a coSpace's secondary URI.)

Upgrade fails because the upgrade image failed to mount

If you are upgrading either the Server deployment or a virtualized deployment, and see an error message that the upgrade image failed to mount, check the settings on the tool used to transfer the file. If you are using WinSCP ensure that the transfer setting is 'binary' not 'text'. Using the incorrect setting results in the transferred file on both the VmWare and server being slightly smaller than the original size – and this prevents successful upgrade.

Tips for making Multiway calls

If you are confident that your VCS settings are correct, try both of the following:

- Disable H.323 on the Cisco endpoints (either the endpoint is not registered with H.323 or H323 is disabled on the endpoint)
- Ensure that the Multiway address on the endpoints is prefixed with "sip:" e.g. sip:<multiway uri>

Does the Acano solution support multiple domains?

The Call Bridge can currently support coSpaces on many SIP domains, but in the current software release the XMPP server only supports a single domain. Therefore if users want to log in with Acano clients they must all be on the same domain. While it is possible to change the XMPP domain, this will mean that your existing clients will be unable to login. We are planning to enable support for multiple XMPP domains in the future.

Troubleshooting Web Bridge connectivity issues

To troubleshoot Web Bridge connectivity issues:

1. On an Acano PC Client or Mac Client try to sign in using the credentials of a user on the Acano solution.

   If this fails with the error message "Unable to connect to the Acano Server - try again later", this suggests that there is a problem in the connectivity between the Web Bridge and the XMPP server. When a user tries to log in to the Web Bridge with a user name of the form user1@example.com, the Web Bridge performs a DNS SRV lookup of _xmpp-client._tcp.example.com in order to discover the IP address of the XMPP server. If the Web Bridge cannot resolve this DNS record, the login fails with the error message above. This can be tested.

2. SSH to the server running the Web Bridge and issue the following command:

   `dns app lookup SRV _xmpp-client._tcp.example.com` on an Acano X series server

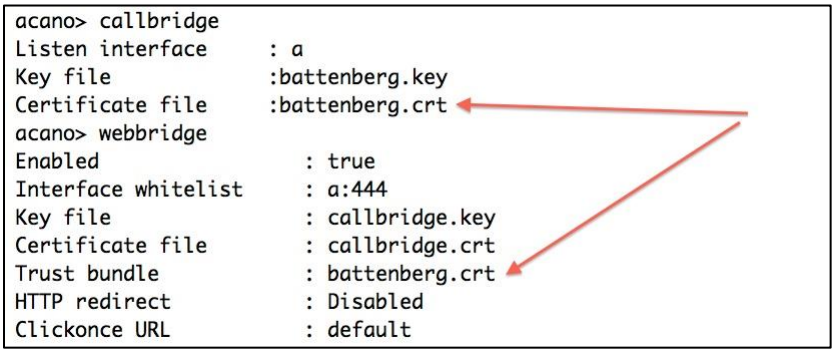
   or

   `dns lookup SRV _xmpp-client._tcp.example.com` (on a virtualized deployment)

   This command returns the IP address of your XMPP server.

If a user can log in and join a call but a guest cannot, this suggests that there is a problem with the HTTPS connection between the Call Bridge and Web Bridge. If this is the case, you see an error when trying to join as guest saying that the WebRTC client is unable to connect to Acano solution. In this case:

1. Log in to the Call Bridge Web Admin Interface and go to **Configuration >General**.
2. In the Web Bridge Settings section, check that the Guest Account Client URI is the same address that which users put in their browser to when logging in (accessing the Web Bridge).
3. If this is, then verify that the Web Bridge has been set up to trust the Call Bridge's SSL certificate by entering the `callbridge` command in the MMP of the server it is running on.



   a. If this is not the case issue the command:

      `webbridge trust <cert.crt>`

      where cert.crt is replaced by the name of the Call Bridge certificate.

Note: If you are using a split deployment, SSH to the Core and Edge servers separately, to ensure that the Certificate file for the Call Bridge is listed as the trust bundle for the Web Bridge.

If this is not the case, copy the Call Bridge certificate to the Edge server and then configure the Web Bridge to trust the Call Bridge using the command above.

I see following error message when trying to add a Call Bridge: "Parent IM domain <example.com> of domain <callbridge.example.com> does not exist". What is wrong?

This message usually indicates that the XMPP domain has changed and therefore the XMPP server needs to be reset.

1. Disable the XMPP server, reset it and then enable the XMPP server as follows:

```
xmpp disable
xmpp reset
xmpp enable
```

2. Try to add the Call Bridge again with the command

```
xmpp callbridge add callbridge
```

3. If you see the following error, reboot the Core server:

```
xmpp callbridge add callbridge
Error
Waiting for XMPP configuration daemon to connect
```

How do I set up “Lecture mode”?

While there is no Lecture mode as such in the Acano solution, from R1.2 the new profiles allow you to assign settings to different URI's.

For example, you can create a "Presenter" URI such that calls to this URI will always be unmuted and take the large window. Similarly, a "Guest" URI can be created that will mute calls by default. For example:

- Presenter: Dial URI 5500@example.com, equal layout, all participants visible, no mic mute
- Guest: Dial URI 5600@example.com, speaker large (to show presenter), mic mute, if no Presenter in call - video and audio is not sent

To achieve this, follow this API example:

1. Create a coSpace with the name Lecture Mode with Profiles
2. Create the Presenter Mode Call Leg Profile:
   POST https://example.com/api/v1/callLegProfiles defaultLayout=allEqual
3. Create the Guest Mode Call Leg Profile:
   POST https://
   example.com/api/v1/callLegProfilesneedsActivation=true&defaultLayout=speakerOnly&rxAudioMute=true&deactivationMode=deactivate
4. Get the Call Leg Profile IDs:
   GET https:// example.com/api/v1/callLegProfiles
   Presenter Call Leg Profile ID: 360b40bf-4c7d-41ff-a355-496c0e720649
   Guest Call Leg Profile ID: 5546a47f-262a-4399-a799-0a03ddc2c66c
5. Get the coSpace ID:
   GET https://example.com/api/v1/coSpaces
   coSpace ID: 83b4f7d0-ffb7-4fbc-83c0-91ebe04f2af3
6. Create the Presenter Mode Access Method tied to URI and Call ID 5500:
   POST https:// example.com/api/v1/coSpaces/83b4f7d0-ffb7-4fbc-83c0-91ebe04f2af3/accessMethodsuri=5500&callLegProfile= 360b40bf-4c7d-41ff-a355-496c0e720649&callID=5500
   (Access Method ID: f3a7cf1a-961f-4fec-b19d-5db558851305)
7. Create the Guest Mode Access Method tied to URI and Call ID 5600:
   POST https:// example.com/api/v1/coSpaces/83b4f7d0-ffb7-4fbc-83c0-91ebe04f2af3/accessMethodsuri=5600&callLegProfile=5546a47f-262a-4399-a799-0a03ddc2c66c&callID=5600
   (Access Method ID: 056a58ee-12bc-404f-b863-834cba4707db)

For a full description of the API methods and the features that can be set for each profile see the API Reference for R1.2.

How do I set up host and guest access?

An accessMethod is a way of adding additional ways for users to dial in to a coSpace with associated callLegProfiles that apply a certain configuration to the participant. One classic example of this is to set up a host/guest configuration so that depending on what URI & passcode is used participants are either assigned the 'host' profile or the 'guest' profile which might make them wait for a host to join the meeting before their own call leg is activated and then they are disconnect when the host leaves (for example).

One way to implement this is to use the coSpace URI for the guest(s) and assign a 'guest' callLegProfile to the coSpace. Then use the API to add an accessMethod which defines the URI for the host(s) to dial in to and associate a callLegProfile with it. For example:

Action	Method	URI	Body data	Result
Create host callLegProfile	POST	https://acanoServer/api/v1/callLegProfiles	defaultLayout=True	callLegProfile with id 93e6ec12-44f6-4a29-ad3b-6eebe1cfd917 is created
Create guest callLegProfile	POST	https://acanoServer/api/v1/callLegProfiles	needsActivation=true& defaultLayout=speakerOnly& rxAudioMute=true& deactivationMode=deactivate	callLegProfile with id 6eebbc8c-c69c-43f0-8f5d-2349837839a2 is created
Associate guest callLegProfile with coSpace	PUT	https://acanoServer/api/v1/coSpaces|/<coSpace ID>	callLegProfile=6eebbc8c-c69c-43f0-8f5d-2349837839a2	Guest profile is used when coSpace URI is dialed
Create host accessMethod on coSpace	POST	https://acanoServer/api/v1/coSpaces/<coSpace ID>/accessMethods	uri=20991&callLegProfile=93e6ec12-44f6-4a29-ad3b-6eebe1cfd917&callID=20991	Users can dial 20991 to access the coSpace with host privileges

Because the guest callLegProfile has needsActivation=True, any guest's call leg will not be started until a participant who does not have needsActivation enabled joins the coSpace; in this case a participant using the host callLegProfile.

How do I enforce encryption for a coSpace?

You need to use the API:

1. Create a calLegProfile and set the parameter sipMediaEncryption to required.
   a. Use the POST method, e.g. to https://<server IP address>/api/v1/callLegProfiles, with the body as sipMediaEncryption=required.
2. Find the ID of this new callLegProfile.
   a. Use the GET method, e.g. to https://<server IP address>/api/v1/callLegProfiles.
3. Find the ID of the coSpace that you want to enforce encryption on.

a. Use the GET method to https://<server IP address>/api/v1/coSpaces.

4. Associate the CallLegProfile with the coSpace.
   a. Use the PUT method to https://<server IP address>/api/v1/cospaces/<coSpace_ID>, with the body as callLegProfile=<callLegProfile_ID>

Encryption is now enforced on all calls in this coSpace. (You can also enforce encryption at tenant level or associate it with access methods.)

I see that different members of the same coSpace can have different permissions on that coSpace. How does this occur?

From R1.2 members of a coSpace can have the following permissions set either automatically or manually. The default permissions for users depend on the way in which they become a member.

- When adding or modifying a coSpace member via the API you can set/update the following (see the API Reference for details) without any cross-dependencies or limitations:
  - canDestroy
  - canAddRemoveMember
  - canChangeName
  - canChangeUri
  - canChangeCallId
  - canChangePasscode
  - canPostMessage
  - canRemoveSelf
- From an Acano client (depending on client type and version) members with canAddRemoveMember set to true can add other users as members of the coSpace. New members have identical permissions to the member who added them, except in one case: when the original member also has canRemoveSelf set to false.

  Members who cannot remove themselves from the coSpace (as controlled by canRemoveSelf) should not be able to create a second member in order to delete their own membership. Therefore any member created from an Acano client by another member in this situation will have canAddRemoveMember set to false and canRemoveSelf set to true. All other permissions are copied from the original member.
- Auto-generated members (created by an LDAP sync) have auto-generated permissions because it makes no sense to allow them to make changes that will be overwritten by the next LDAP sync. Therefore, for these users the following parameters are always set to false: canDestroy, canChangeName, canChangeUri, canChangeCallId and canRemoveSelf. The other “can” parameters above are set to true. Note that changing any of these settings for an auto-generated member via the API will only have a temporary effect and will be overwritten at the next LDAP sync.
- If a user creates a coSpace from the Acano client, then all members get all permissions (all “can” parameters above are set to true by default.

How do I set the default layout for every coSpace?

Set the defaultLayout in a callLegProfile and apply that callLegProfile at the system (global) level. Note that this default layout will only apply if the setting is not overwritten by a layout setting at a lower level e.g. per coSpace.

What information is included in the email invitation?

If you invite a participant from an Acano client, either from the coSpace information panel or when in a call, only the details displayed in the coSpace's information panel are included in the email. Any calling details in an access method on the coSpace are not included.

What does "RTCP unprotect authentication failure" in the event log mean?

RTCP unprotect authentication failures aren't anything to worry about on their own; they are the result of authentication failures on incoming RTCP, which is mostly due to 3rd party endpoints not following the specifiction for this correctly.

How do I move the master database?

This FAQ applies to Acano solution R1.6 onwards only.

The master database in a cluster will move automatically if the current master goes down, but you cannot control which of the previous standby databases will become the new master database for the cluster. The following procedure should only be used if you want to move the master database to a particular host server; but of course the master database will move again automatically if this server goes down.

Note: The process to move the master database described below causes all active calls hosted on Call Bridges connected to the database cluster to drop; therefore only perform this procedure during a scheduled down time.

---

1. Check that the status of all the standby databases in the cluster is "In sync" by running the following MMP command on all servers hosting one of these databases.

   ```
   dbcluster status
   ```

2. Uncluster all the databases by running the following MMP command on all servers including that hosting the master database.

   ```
   dbcluster disable
   ```

   Note: All active calls will drop.

   ---

3. On the server with the database that you want to be the master, initialize the database by running the following MMP command:

   ```
   dbcluster initialise
   ```

4. Attach the other databases to the master by running the following MMP command:

   ```
   dbcluster attach <master hostname/IP>
   ```

5. Check the status of the new cluster to make sure that all the databases are in sync and to check which is the master database.

   ```
   dbcluster status
   ```

Does Acano support Skype integration?

The Acano Solution R1.6 supports audio, IM and presence between Skype users and the Acano system. This allows:

- Skype users to join coSpaces
- Skype users to make point-to-point calls to non-Skype users (Acano/SIP/WebRTC...) using the Acano solution as a gateway
- Non-Skype users to make point-to-point calls to Skype users (using the Acano solution as a gateway)
- Skype users to add coSpaces or non-Skype users to their Contact list and see presence
- Acano users to dial out to Skype users to invite them into a coSpace
- Chat between a coSpace and a Skype user

This feature requires configuration of Skype to Lync integration so that the call will come through your Lync Edge server. To configure Skype integration, you must provision details of the Acano server (or the Acano Edge server in split deployment) and your domains on Microsoft's systems. For more details see:

- http://products.office.com/en-us/Lync/lync-skype-connectivity .
  http://technet.microsoft.com/en-us/library/dn440174.aspx .
  http://technet.microsoft.com/en-us/library/dn440173.aspx .
  http://technet.microsoft.com/en-us/library/dn440175.aspx .

To add an Acano address as Skype contact, in the Skype client enter the URI (e.g. mycospace@example.com) in the Search box, then click **Search Skype**. The contact will show as a Lync user after it has found (this might take a while) and then you can call it from your Skype client.

We plan to support video but we require Microsoft to add this to their Lync-Skype integration first.

Currently you cannot invite a Lync user to a Skype group call—a limitation of using Microsoft's Lync-Skype integration.

What is the minimum bit rate for audio and video?

For any type of connection (e.g. Acano client, SIP, Lync, WebRTC) even though in theory a 128kbps connections should allow both audio & video, we recommend at least 256kbps for an acceptable user experience.

Is TIP supported in R1.6 and on what systems?

TIP is supported from R1.6, allowing you to make calls, to and accept calls from, both single- and triple-screen TIP devices. These calls support both presentation and encryption, and in the case of triple-screen systems, new layouts are used that span all three screens.

Enable TIP support in the Web Admin Interface: go to **Configuration > Call Settings** and set TIP (Telepresence Interoperability Protocol) Calls to Enabled. Then set both SIP Bandwidth Settings to at least 4000000.

Currently only Cisco CTS and TX systems running TIPv8 are supported. Equipment from other vendors has not been tested. If your CTS or TX system is using an earlier version of TIP then it will need to be upgraded.

In release 1.6, can I have one Edge server for two Core servers?

Yes, you can use one Edge server for two Core servers, **but only** if they are part of a Call Bridge cluster i.e. using a common coSpace database and the same software version.

4 Virtualized Deployments

What VM host server should I use?

A qualified host server with some specific resources. See the Acano solution Virtualized Deployment Installation Guide for the latest details. The Acano solution will not run or will give very poor service on older virtualized hosts.

Which versions of the hypervisor are recommended?

The only qualified host is described in the Acano Solution Virtualized Deployment Installation Guide. It is a Dell R620 with ESXi hypervisor version 5.0 or 5.1.

We do not recommend or support other versions e.g. v5.5. The virtualized deployment can run on Hyper-V 2012 but it's not supported and you would need to convert the OVF to Hyper-V format using Microsoft's "Virtual Machine Migration tool".

© 2015 Acano (UK) Ltd. All rights reserved.
This document is provided for information purposes only and its contents are subject to change without notice. This document may not be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without our prior written permission.

Acano and coSpace are trademarks of Acano. Other names may be trademarks of their respective owners.